Consumer Data Privacy & Security Legislation

A Legislative Scan to Assess State-Level Protections for Patient Generated Health Data

Overview

The Maryland Health Care Commission (MHCC) examines trends in health care data breaches reported by covered entities[1] and business associates[2] in Maryland and the nation and a changing cybersecurity landscape, which includes risks associated with patient generated health data (PGHD).[3, 4] PGHD is health-related data[5] created and recorded by or from patients or family members/caregivers outside of a clinical setting using consumer health technologies and third-party applications.[6] This rapidly growing segment of health care presents unique pathways to help consumers better manage their health and participate in their health care.[7]

Gaps exist in the advancement of technology and existing legal framework for the privacy and security of electronic health information.[8] In many instances, PGHD is not protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), presenting risks to consumers who may intentionally or unintentionally share their health-related data. Consumer health technologies that lack HIPAA-equivalent protections can result in selling or sharing PGHD without users' consent or knowledge, differences in breach response, and re-identifying PGHD (if proper security measures to de-identify data are not in place). To reduce the risk of unauthorized access and cyber threats, some states have passed legislation aimed at protecting consumer data, including health-related data that falls outside the bounds of HIPAA; other states are beginning to explore legislation.[9]

About the Legislative Scan

The MHCC conducted a legislative scan (scan) to identify states with consumer data privacy laws that include protections for PGHD that is not subject to HIPAA protections. Approximately 12 states, including Maryland, have passed consumer data privacy laws, with four new states passing legislation since 2021; some legislation includes protections for genetic data that is generated when testing is conducted outside of a clinical setting using direct-to-consumer genetic testing companies.[10] These companies provide services to make predictions about health, provide information about common traits, and offer clues about a person's ancestry.[11]

Most laws impose transparency and notice requirements on businesses that collect, sell, or share personal information.[12] In general, state-level protections give consumers the right to know how and with whom their data is used, shared, or sold, as well as the right to opt-in, opt-out, or restrict the selling and sharing of personal information. Other protections require technology vendors[13] to implement certain security safeguards (e.g., regular risk assessments).

Table 1 provides a high-level snapshot of the key categories for protections by state and the enactment and effective dates for each law. **Table 2** includes detailed information as it relates to applicability and specific privacy and security provisions.

Table 1: Key Categories – State-Level Privacy and Security Protections *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*						
General Information	**Consumer Privacy Requirements/Rights**				**Security Safeguards/Business Requirements**	
State/Statute	**Know How/Why/Who Has Access**	**Portability[14]**	**Correct and/or Delete**	**Opt-In or Opt-Out of Selling and/or Sharing Data**	**Transparency/ Notice Requirements**	**Security Controls**
California Consumer Privacy Act (CCPA) Enacted 2018 | Effective 1/1/20	✔		✔	✔	✔	✔
California Privacy Rights and Enforcement Act (CPRA) Enacted 2020 | Effective 1/1/23	✔	✔	✔	✔	✔	✔
California Internet of Things Cybersecurity Improvement Act of 2017 Enacted 2018 | Effective 1/1/20						✔
California - Privacy: Mental Health Digital Services: Mental Health Application Information Enacted 2022 | Effective 9/28/22	✔			✔	✔	✔
Colorado Privacy Act Enacted 2021 | Effective 7/1/23	✔	✔	✔	✔	✔	✔
Connecticut Data Privacy Act Enacted 2021 | Effective 7/1/23	✔	✔	✔	✔	✔	✔
Nevada Privacy Law Enacted 2019 | Effective 10/1/19				✔	✔	✔
Vermont Data Broker Regulation Act Enacted 2018 | Effective 1/1/19					✔	✔
Utah Consumer Privacy Act Enacted 2022| Effective 12/31/23	✔		✔	✔	✔	✔
Virginia Consumer Data Protection Act Enacted 2021 | Effective 1/1/23	✔	✔	✔	✔	✔	✔

Table 1: Key Categories – State-Level Privacy and Security Protections *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*						
General Information	**Consumer Privacy Requirements/Rights**				**Security Safeguards/Business Requirements**	
State/Statute	**Know How/Why/Who Has Access**	**Portability[14]**	**Correct and/or Delete**	**Opt-In or Opt-Out of Selling and/or Sharing Data**	**Transparency/ Notice Requirements**	**Security Controls**
Arizona Genetic Information Privacy Act (GIPA)* Enacted 2021 | Effective 9/29/21	✔		✔	✔	✔	✔
California Genetic Information Privacy Act (GIPA)* Enacted 2021 | Effective 1/1/22	✔		✔	✔	✔	✔
Florida Protecting DNA Privacy Act* Enacted 2021 | Effective 10/1/21				✔		
Kentucky Genetic Information Privacy Act* Enacted 2022 | Effective 6/1/22	✔		✔	✔	✔	✔
Maryland Genetic Information Privacy Act* Enacted 2022 | Effective 10/1/22	✔		✔	✔	✔	✔
Utah Genetic Information Privacy Act (GIPA)* Enacted 2022 | Effective 5/5/21	✔		✔	✔	✔	✔
Wyoming Genetic Information Privacy Act* Enacted 2022 | Effective 7/1/22	✔		✔	✔	✔	✔

Table 2: Applicability and Key Provisions in Law

PGHD and Genetic Data

Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)

General Information		Consumer Privacy Requirements/Rights	Security Safeguards/Business Requirements
State/Statute	**Applicability**	**Key Provisions**	**Key Provisions**
California Consumer Privacy Act (CCPA) Enacted 2018 Effective 1/1/20	Businesses w/gross annual revenue over $25 million; or buy, receive, or sell the personal information of 50,000 or more California residents; or derive 50% or more of annual revenue from selling California residents' personal information Does not apply to government or nonprofit organizations	• May ask businesses to disclose what personal information they have about them and what they do with that information, to access and delete personal information, and opt-out of personal information being sold • Children 13-16 must opt-in for sale of their personal information; children under 13 must have a parent opt-in for sale of their personal information • Consumers have private right of action for data breaches	• Businesses must provide consumers with a privacy policy stating what personal data they collect, what they do with it, how consumers can exercise their rights, and what personal data is shared with third parties. • Must include a "Do Not Sell My Personal Information" link on the homepage of their website and cannot require users to create an account before opting-out • Must implement reasonable security measures
California Privacy Rights and Enforcement Act (CPRA) of 2020 – Proposition 24 (Updates, modifies, and expands rules stipulated by CCPA) Enacted 2020 Effective 1/1/23	Changes threshold number of consumers or households from 50,000 to 100,000 Extends applicability to businesses that share (not just sell) personal information	• In addition to rights granted in CCPA, California residents can opt-out of sharing personal information for targeted marketing, profiling, or automated decision making; includes the right to correct personal information and obtain a copy in reasonable format (portability) • Includes right to limit use and disclosure of *sensitive information,* which includes health and genetic information	• In addition to CCPA obligations, businesses must post "Do Not Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links • Consent is not legitimate if obtained through dark patterns[15] • Must submit regular risk assessments to the newly established California Privacy Protection Agency
California Internet of Things Cybersecurity Improvement Act of 2017 Enacted 2018 Effective 1/1/20	Manufacturers of any device (sold or offered for sale in California) that can connect to the internet and are assigned an IP or Bluetooth address; includes personal fitness devices, medical devices, televisions, printers, appliances, etc.	None	• Requires all "connected devices" sold or offered for sale in California to have a reasonable security feature, which meets one of the following requirements: (1) The preprogrammed password is unique to each device manufactured; or (2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time[16]

Table 2: Applicability and Key Provisions in Law *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*			
General Information		**Consumer Privacy Requirements/Rights**	**Security Safeguards/Business Requirements**
State/Statute	**Applicability**	**Key Provisions**	**Key Provisions**
California - Privacy: Mental Health Digital Services: Mental Health Application Information Amends Confidentiality of Medical Information Act (CMIA) Enacted 2022 Effective 9/28/22	Any business that offers a mental health digital service to a consumer for the purpose of allowing the individual to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition (e.g., a health and wellness app that asks users to record anxiety symptoms)	• Deems businesses that provide digital mental health as health care providers for purposes of the CMIA and thus subject to provisions in CMIA • CMIA prohibits health care providers from sharing, selling, using for marketing, or otherwise using any medical information for purposes not necessary to provide health care services without the consumer's signed authorization	• Businesses that partner with health care providers (e.g., licensed mental health therapists) must disclose to the providers information regarding how to find data breaches reported to the Attorney General pursuant to Section 1798.82
Connecticut Data Privacy Act Enacted 2022 Effective 7/1/23	Data controllers that conduct business in Connecticut and process the personal data of at least 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing payment transactions; and/or or at least 25,000 consumers and derived over 25% of their gross revenue from the sale of personal data	• Connecticut residents can opt-out of sale of personal information and opt-out of sharing personal information for targeted marketing, profiling, or automated decision making • Must consent to sharing or selling sensitive information, which includes health and genetic information	• Controllers must implement a universal opt-out mechanism for targeted advertising and sale of personal data on their website by 1/1/25 • Must conduct and document a data protection assessment for each of the processing activities that presents a heightened risk of harm to a consumer, which includes processing for targeted advertising, for sale of personal data, for profiling, and any processing of sensitive data • Must provide consumers with a privacy policy stating what personal data they collect, what they do with it, how consumers can exercise their rights, and what personal data is shared with third parties

Table 2: Applicability and Key Provisions in Law *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*			
General Information		**Consumer Privacy Requirements/Rights**	**Security Safeguards/Business Requirements**
State/Statute	**Applicability**	**Key Provisions**	**Key Provisions**
Colorado Privacy Act Enacted 2021 Effective 7/1/23	Data controllers that conduct business or deliver commercial products in Colorado and process personal data of at least 100,000 consumers during a year; and/or derive revenue or discount on goods/ services from the sale/processing of personal data of at least 25,000 consumers	• Colorado residents can opt-out of sale of personal information and opt-out of sharing personal information for targeted marketing, profiling, or automated decision making • Must consent to sharing or selling *sensitive information,* which includes health and genetic information	• Data controllers must provide consumers with a privacy policy stating what personal data they collect, what they do with it, how consumers can exercise their rights, and what personal data is shared with third parties • Starting 7/1/24, data controllers who collect and sell/use data for targeted marketing must implement universal opt-out mechanism on their website; AG will release technical specification by 7/1/23 • Consent is not legitimate if obtained through dark patterns • Must take reasonable measures to secure personal data compatible with the scope, volume, and nature of the data; must conduct and document data protection assessments
Nevada Privacy Law Enacted 2019 Effective 10/1/19 Amended in 2021 Effective 10/1/21	Online businesses, services, and operators of internet websites that collect and maintain covered information from consumers who reside in Nevada; does not apply to businesses that collect data offline *Amended in 2021 to also include "data brokers" and expand the definition of "sale" of consumer personal data	• Nevada consumers have the right to opt-out of sale of covered information	• Requires businesses to use reasonable security measures to protect data from unauthorized access, acquisition, destruction, use, modification, or disclosure • Only applies to health information (that is not protected by HIPAA) when it is sold to a third-party with another piece of identifying information (name, address, email address, etc.) • Requires businesses to provide an address, toll-free telephone number, or website to submit verified opt-out requests • Businesses must comply with opt-out requests within 60 days

Table 2: Applicability and Key Provisions in Law *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*			
General Information		**Consumer Privacy Requirements/Rights**	**Security Safeguards/Business Requirements**
State/Statute	**Applicability**	**Key Provisions**	**Key Provisions**
Utah Consumer Privacy Act Enacted 2022 Effective 12/31/23	Data controllers or processors that conduct business in Utah or produce a product or service that is targeted to Utah residents, has annual revenue of $25,000,000 or more, and satisfies one or more of the following thresholds: during a calendar year, controls, or processes personal data of 100,000 or more consumers; or derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers *Exempts covered entities and business associates governed by HIPAA, not just PHI collected pursuant to HIPAA	• Utah residents can opt-out of sale of personal information and opt-out of sharing personal information for targeted marketing, profiling, or automated decision making • Right to access, delete (but not correct), or obtain a copy of personal information	• Must provide consumers with a privacy policy stating what personal data they collect, what they do with it, how consumers can exercise their rights, and what personal data is shared with third parties • Must provide consumers "clear notice and an opportunity to opt-out" before processing their sensitive data • Must have verifiable parental consent to process personal data of consumers known to be under the age of 13 are required to process such data in accordance with the Children's Online Privacy Protection Act (COPPA) • The Utah Department of Commerce Division of Consumer Protection is tasked with receiving and investigating consumer complaints before referring to the Utah Attorney General (AG) for enforcement action • Must have "reasonable administrative, technical, and physical security practices to protect personal data collected"
Virginia Consumer Data Protection Act (VCDPA) Enacted 2021 Effective 1/1/23	All persons that conduct business in Virginia and either (1) control or process personal data of at least 100,000 consumers or (2) derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers *Exempts covered entities and business associates governed by HIPAA, not just PHI collected pursuant to HIPAA	• Virginia residents can opt-out of sale of personal information and opt-out of sharing personal information for targeted marketing, profiling, or automated decision making Right to access, correct, delete, or obtain a copy of personal information	• Businesses must provide consumers with a privacy policy stating what personal data they collect, what they do with it, how consumers can exercise their rights, and what personal data is shared with third parties • Prohibits the processing of sensitive data without obtaining the consumer's consent. Processing sensitive data concerning a known child is prohibited without following COPPA • Requires a contract between a controller and processor to govern the processor's data processing procedures • Must have "reasonable administrative, technical, and physical security practices to protect personal data collected"

Table 2: Applicability and Key Provisions in Law *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*			
General Information		**Consumer Privacy Requirements/Rights**	**Security Safeguards/Business Requirements**
State/Statute	**Applicability**	**Key Provisions**	**Key Provisions**
Vermont Data Broker Regulation Act Enacted 2018 Effective 5/22/18 Registration and data security obligations effective 1/1/19	Applies to data brokers--businesses that knowingly collect and license the personal information of consumers with whom such businesses do not have a direct relationship	None	• Data brokers must provide consumers with contact information, how to opt-out of first-party and third-party data collection (if permitted by the business), whether a purchaser credentialing process has been implemented, and if the business experienced security breaches within the last year/number of individuals affected • Data for minors is subject to additional disclosures • Must implement and maintain a written information security program containing administrative, technical, and physical safeguards to protect personally identifiable information (similar to HIPAA security requirements) • Must register annually with the Secretary of State; upon filing, must disclose data breaches within the prior year and number of consumers affected
Arizona Genetic Information Privacy Act (GIPA)* Enacted 2021 Effective 9/29/21	Direct-to-consumer genetic testing companies that collect genetic data from residents of Arizona	Consumers must provide "express consent" for a company to disclose genetic information to third parties (other than the company's vendors or service providers), to use for purposes other than providing the genetic testing product or service to the consumer; or retaining the genetic sample following the initial testing service	• Companies must provide customers with a high-level privacy policy overview • Must provide prominent, publicly available privacy notice that includes information about the company's data collection, consent, use, access, disclosure, transfer, security, retention, and deletion practices • Must develop, implement, and maintain a comprehensive security program to protect genetic data against unauthorized access, use, or disclosure • Requires a valid legal process for disclosing genetic data to law enforcement

Table 2: Applicability and Key Provisions in Law *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*			
General Information		**Consumer Privacy Requirements/Rights**	**Security Safeguards/Business Requirements**
State/Statute	**Applicability**	**Key Provisions**	**Key Provisions**
California Genetic Information Privacy Act (GIPA)* Enacted 2021 Effective 1/1/22	Direct-to-consumer genetic testing companies and other companies that collect, use, maintain, or disclose genetic data collected or derived from a direct-to-consumer genetic testing product or service or directly provided by a consumer	• Requires "informed consent" from consumers regarding the collection, use, and disclosure of their genetic testing • May request that personal information be deleted and biological sample(s) destroyed	• Companies must provide notice on the company's policies and procedures for the collection, use, maintenance, and disclosure of genetic data • Cannot use opt-out or dark patterns for consumer consent • Reasonable security measures must be in place • Must destroy consumer's genetic information within 30 days of the consumer's revocation of consent • May not disclose a consumer's genetic data to any entity that is responsible for making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment (or to entities that advise such companies)
Florida Protecting DNA Privacy Act* Enacted 2021 Effective 10/1/21	Applies to DNA samples collected from any person in Florida, and regulates the use, retention, disclosure, or transfer of such DNA, or of any analysis derived from it	• Consumer must provide "express consent" for any specified use of genetic information	• The law makes the submittal of another person's DNA sample for DNA analysis without that person's express consent a third-degree felony • Disclosure of DNA test results without the person's "express consent" is a third-degree felony[17] • Sale or transfer of another person's DNA sample or DNA test results to a third party without the person's "express consent" is a second-degree felony

Table 2: Applicability and Key Provisions in Law *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*			
General Information		**Consumer Privacy Requirements/Rights**	**Security Safeguards/Business Requirements**
State/Statute	**Applicability**	**Key Provisions**	**Key Provisions**
Kentucky Genetic Information Privacy Act Enacted 2022 Effective 6/1/22	Direct-to-consumer genetic testing companies that collect genetic data from residents of Kentucky	• Consumers have a right to access their genetic data, delete their account and genetic data, and request and obtain the destruction of their biological samples	• Must provide a high-level privacy policy overview; and a prominent, publicly available privacy notice; obtain a consumer's consent for the collection, use, or disclosure of the consumer's genetic data; and require a valid legal process for disclosing genetic data to law enforcement or any other government agency without a consumer's express written consent • May not disclose a consumer's genetic data to any of the following without written consent: (1) an entity offering health insurance, life insurance, disability insurance, or long-term care insurance; or (2) an employer of the consumer
Maryland Genetic Information Privacy Act* Enacted 2022 Effective 10/1/22	Direct-to-consumer genetic testing companies that collect genetic data from residents of Maryland	• Consumers have a right to access their genetic data, delete their account and genetic data, and request and obtain the destruction of their biological samples	• Must provide a high-level privacy policy overview; and a prominent, publicly available privacy notice; obtain a consumer's consent for the collection, use, or disclosure of the consumer's genetic data; and require a valid legal process for disclosing genetic data to law enforcement or any other government agency without a consumer's express written consent • May not disclose a consumer's genetic data to any of the following without written consent: (1) an entity offering health insurance, life insurance, disability insurance, or long-term care insurance; or (2) an employer of the consumer

Table 2: Applicability and Key Provisions in Law *PGHD and Genetic Data* *Laws that are specific to genetic testing information are included at bottom of table and marked with an asterisk (*)*			
General Information		**Consumer Privacy Requirements/Rights**	**Security Safeguards/Business Requirements**
State/Statute	**Applicability**	**Key Provisions**	**Key Provisions**
Utah Genetic Information Privacy Act (GIPA)* Enacted 2021 Effective 5/5/21	Direct-to-consumer genetic testing companies that collect genetic data from residents of Utah	• Delete and request biological sample(s) to be destroyed. • Separate "express consent" is required for: (1) transfers or disclosures of genetic data to any person (other than vendors); (2) use of the information beyond the primary purpose of the genetic testing; or (3) retention of the biological sample(s) following completion of the initial testing service; and (4) third party marketing activities	• Companies must provide prominent, publicly available privacy notice that includes information about the company's data collection, consent, use, access, disclosure, transfer, security, retention, and deletion practices • Must develop, implement, and maintain a comprehensive security program to protect consumer's genetic data against unauthorized access, use, or disclosure • Companies with a first party relationship may, without "express consent," provide customized content or offers on the company's website or through the app/service • Requires a valid legal process for disclosing genetic data to law enforcement • Cannot disclose genetic data to a health insurance company or an individual's employer without "express consent"
Wyoming Genetic Information Privacy Act* Enacted 2022 Effective 7/1/22	Direct-to-consumer genetic testing companies that collect genetic data from residents of Wyoming	• Consumers have a right to access their genetic data, delete their account and genetic data, and request and obtain the destruction of their biological samples	• Must provide a high-level privacy policy overview and a prominent, publicly available privacy notice; obtain a consumer's consent for the collection, use, or disclosure of the consumer's genetic data; and require a valid legal process for disclosing genetic data to law enforcement or any other government agency without a consumer's express written consent • May not disclose a consumer's genetic data to any of the following without written consent: (1) an entity offering health insurance, life insurance, disability insurance, or long-term care insurance; or (2) an employer of the consumer

At least 29 states and the District of Columbia proposed consumer privacy bills in 2022 or carried over legislation from 2021, demonstrating that many states are beginning to explore legislation that could ensure minimum safeguards for PGHD that fall outside the scope of HIPAA.[18] Bills that did not pass are excluded from the table. Approximately 22 states (including Maryland) have breach notification laws that include health information in their definition of personal information.[19] At the federal level, the Health Breach Notification Rule[20] requires entities not covered by HIPAA (i.e., personal health record vendors and related entities) to inform consumers about unauthorized disclosures of PHI.[21] The Federal Trade Commission (FTC) is tasked with enforcement of the Health Breach Notification Rule.[22]

For more information on privacy and security risks and the current state of health care cybersecurity, visit: mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Patient_Generated_Health_Data_20211109.pdf.

---

[1] Covered entities include health plans, health care clearinghouses, health care providers, and business associates.
[2] Business Associates include entities that create, receive, maintain, or transmit PHI on behalf of covered entities or another business associate.
[3] Data is obtained from the U.S. Department of Health and Human Services, Office for Civil Rights for breaches affecting 500 or more individuals. The OCR breach portal is available at: ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
[4] MHCC reports on health care data breach trends available at: mhcc.maryland.gov/mhcc/Pages/hit/hit_cybersecurity/hit_cybersecurity.aspx.
[5] Examples include blood glucose monitoring or blood pressure readings using home health equipment, exercise and diet tracking using a mobile application, and questionnaires, such as screening, medication adherence, risk assessment, and intake. More information is available at: www.healthit.gov/sites/default/files/patient_generated_data_factsheet.pdf.
[6] ONC, *Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024*, January 2018. Available at: www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf.
[7] *Ibid.*
[8] Perspectives in Health Information Management, *Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply*, December 2020. Available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC7883355/.
[9] National Conference of State Legislatures, *2021 Consumer Data Privacy Legislation*. Available at: www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx.
[10] Direct-to-consumer genetic testing companies generally request the consumer collect a specimen, such as saliva or urine, and send it to the company for testing and analysis of their DNA (or genome). Results are used for a variety of purposes, such as predicting risk of developing certain diseases, identifying potential medication or diet intolerances, and exploring genetic ancestry. More information is available at: www.fda.gov/medical-devices/in-vitro-diagnostics/direct-consumer-tests.
[11] Direct-to-consumer raw genetic data and third-party interpretation services: more burden than bargain? Moscarello, Tia et al. Genetics in Medicine, Volume 21, Issue 3, 539 - 541
[12] Notice/transparency requirements generally include categories of data processed; purpose of the processing; how, why, and with whom data will be shared; and instructions to exercise consumer rights.
[13] Includes data brokers, online businesses and applications, and manufacturers of consumer health technologies.
[14] Portability refers to the right for a consumer to request their personal information be shared in a common file format.
[15] Dark patterns are defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice." More information is available at: www.jdsupra.com/legalnews/beware-dark-patterns-what-are-they-and-9462310/.
[16] The legislation was prompted by what the bill's sponsor viewed as a lack of security features on internet connected devices that did not already fall under federal regulation, such as those imposed by the FDA or OCR. More information is available at: www.jdsupra.com/legalnews/california-passes-first-of-its-kind-law-93889/.
[17] A law enacted in 2020, Florida HB 1189 (Genetic Information for Insurance Purposes), specifically prohibits use/disclosure of genetic information for life, disability, and long-term care insurance. More information is available at: www.flsenate.gov/Session/Bill/2020/1189#:~:text=Genetic%20Information%20for%20Insurance%20Purposes%3B%20Prohibits%20life%20insurers%20%26%20long%2D,genetic%20information%20for%20any%20insurance.
[18] States include: AK, AZ, CT, DC, FL, GA, HI, KY, LA, IA, IN, MA, MD, ME, MI, MN, MS, NJ, NY, NE, NC, OH, OK, RI, PA, UT, VT, WA, WI, WV. Seventeen states included provisions for regular security risk assessment or other security related processes: CT, HI, IA, IN, KY, LA, MA, MI, MN, NC, NE, NJ, NY, OK, PA, WA, WI. More information is available at: iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

[19] Venable, *Newest Trends in Health Data Breaches: FTC, OCR, and AG Enforcement*, May 2021. Available at: www.venable.com/-/media/files/events/2021/05/newest-trends-in-health-data-breaches.pdf.

[20] Health Breach Notification Final Rule was enacted as part of the American Recovery and Reinvestment Act of 2009. More information is available at: www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf.

[21] The Rule preempts contradictory state breach notification laws, but not those that impose additional – but non-contradictory – breach notification requirements (e.g., state laws that require breach notices to include advice on monitoring credit reports or contact information for consumer reporting agencies). More information is available at: www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule.

[22] FTC enforcement began on February 22, 2010.